

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ABBY LINEBERRY, et al.,
Plaintiffs,
v.
ADDSHOPPER, INC., et al.,
Defendants.

Case No. 23-cv-01996-VC

**ORDER GRANTING IN PART,
DENYING IN PART ADDSHOPPERS'
AND PEET'S COFFEE'S MOTION TO
DISMISS THE FIRST AMENDED
COMPLAINT**

Re: Dkt. Nos. 138, 139

The motion to dismiss is granted in part and denied in part. This ruling assumes the reader is familiar with the facts, the applicable legal standards, the arguments made by the parties, and this Court's prior order on the defendants' first motions to dismiss. *See McClung v. AddShopper, Inc.*, No. 23-CV-01996, 2024 WL 189006 (N.D. Cal. Jan. 17, 2024).

1. *Article III Standing.* The defendants reraise their argument that the plaintiffs have not suffered an injury-in-fact. The prior order explained that "misappropriating a person's browsing activity across a network of thousands of online retailers and using it to barrage that person's devices with unwanted email communications" is "the type of intrusion on privacy and seclusion that can be vindicated in the federal courts." *Id.* at *1. As a reminder, the "question whether an invasion of privacy is severe enough to confer liability is distinct from whether the injury is concrete and particularized enough to confer standing in federal court." *Id.*; *see also TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021); *In re Facebook, Inc., Consumer Privacy User Profile Litigation*, 402 F. Supp. 3d 767, 786 (N.D. Cal. 2019).

The defendants argue that neither Cordero nor Lineberry disclosed private information on

the Peet’s website such that they suffered an injury to their privacy. Whether browsing activity is private or personal enough depends on the facts of each case, including how much information is captured and how it is aggregated or used. Here, as discussed before, the complaint alleges that Addshoppers’ scheme is to “tie browsing activity on one site with personal information disclosed on another site, obviating the need for the retailers to do it themselves.” *Id.* at *2 n.1; *see also* First Amended Complaint ¶¶ 37–38, Dkt. No. 135 (describing how AddShoppers’ “business model hinges on its ability to send targeted emails to individuals who never voluntarily provided their email address to a member of the Data Co-Op”). And the information was not just from one retailer or on one occasion; Addshoppers aggregated browsing activity that spanned across many retailers and over years. In this situation, the plaintiffs have alleged a privacy injury sufficient to confer Article III standing.

The defendants also argue that Cordero lacks standing because he did not allege receiving any targeted emails. Receipt of an unwanted email isn’t necessary to plead a concrete privacy injury. For instance, the common-law tort of intrusion upon seclusion doesn’t require that the private information taken be used in any particular way. *See* Restatement (Second) of Torts § 652B cmt. a, b (1977) (intrusion upon seclusion includes “examination into his private concerns” without “publication or other use of any kind” of the information acquired). Similarly, the common-law tort of publicity given to private life requires that private information be disseminated—akin to Addshoppers disseminating its dossiers to its retailer-customers—but does not require a further intrusion like an email toward the plaintiff. *Id.* § 652D. Therefore, Cordero’s allegation that his browsing activity was tracked by dozens of companies through SafeOpt over several years is sufficient.

2. *CDAFA*. The defendants next argue that the plaintiffs lack statutory standing to bring their CDAFA claims because they have not suffered the type of “damage or loss” necessary under CDAFA. Cal. Penal Code § 502(e)(1). The prior order held that the plaintiffs had adequately alleged damage or loss under a benefit of the bargain theory. *See AddShopper, Inc.*, 2024 WL 189006, at *2. But the plaintiffs removed that theory in their amended complaint, and

now solely rely on the theory that plaintiffs suffered economic loss because the defendants' misappropriation of their data decreased the value of that data. The prior order expressed skepticism of this theory, but the Court now addresses it in more detail. *Id.* at *2.

To begin, the defendants contend that “damage or loss” under CDAFA is limited to damage or loss to a computer system, network, program, or data contained on that computer, as some courts have held. *See Heiting v. Taro Pharmaceuticals. USA, Inc.*, 709 F. Supp. 3d 1007, 1020 (C.D. Cal. 2023). This narrow interpretation of “damage or loss” is not supported by the text of CDAFA. The statute does not define “damage or loss” and the plain reading of “damage or loss by reason of a violation” of CDAFA is that any loss due to the CDAFA violation is cognizable. *See* Cal. Penal Code § 502(e)(1). The statute says that damages “shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access,” but that statement is best read as ensuring one type of damage is cognizable, not limiting damages to that alone. The defendants next point to the federal counterpart to CDAFA, the Comprehensive Computer Data Access and Fraud Act, which also requires “damage or loss” and defines that phrase as limited to “impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). The problem with this analogy is that CDAFA does not have a similar definition for “damage or loss,” and the defendants did not point to any statutory language or legislative history indicating the California Legislature wanted to adopt the federal definition, or even model the state statute after the federal one.

Thus, the plaintiffs may allege damage or loss from the misappropriation of their data, so long as they articulate that theory of loss a concrete way. In this case, the plaintiffs have not done so. The complaint asserts that the plaintiffs suffer an economic loss every time their data is used and shared. Compl. ¶ 73. But they don't provide any allegations about how or why that is the case. For instance, the complaint neither alleges that there is a market for individual people's browsing activity, nor anything about what the actual value of the plaintiffs' data could be. *Cf.*

Brown v. Google LLC, 685 F. Supp. 3d 909, 940 (N.D. Cal. 2023) (holding that plaintiffs alleged CDAFA loss when they alleged Google had a program where it paid users \$3/day for their browsing history). The complaint also doesn't explain whether a person can still sell their data if Addshoppers already has it, nor how the value of a person's data decreases when their data is misappropriated.

The plaintiffs analogize to the intellectual property context and argue that data is like a patent or copyright: it is non-rivalrous, but the patent or copyright holder can still seek damages for reasonable royalties. But patents and copyrights are exclusive rights and others are precluded by statute from using the patented or copyrighted work; in contrast, it's not clear whether each plaintiff has the exclusive right to their data nor is the scope of such an exclusive right clear if it does exist.

This is not to say that a theory of economic loss based on the misappropriation of personal data is never cognizable. But at least here, the complaint fails to allege that the plaintiffs' losses are anything other than "purely hypothetical." *In re Facebook, Inc.*, 402 F. Supp. 3d at 784 (dismissing similarly speculative economic loss theory on Article III standing). The CDAFA claims are dismissed for lack of CDAFA statutory standing.

3. *Plaintiff Cook's Claims Against Peet's*. Peet's argues that Cook's claims must be dismissed because neither CDAFA nor CIPA apply extraterritorially. A California statute applies extraterritorially only if that "intention is clearly expressed or reasonable to be inferred 'from the language of the act or from its purpose, subject matter or history.'" *Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1207 (2011) (quoting *Diamond Multimedia Systems, Inc. v. Superior Court*, 19 Cal. 4th 1036, 1059 (1999)). Here, both CDAFA and CIPA contain language suggesting the statutes only apply in California. *See* Cal. Penal Code § 630 (stating the legislature "intends to protect the right of privacy of the people of this state"); Cal. Penal Code § 502(a) (declaring CDAFA "vital to the protection of the privacy of individuals . . . within this state").

To be sure, as the plaintiffs argue, a California statute may apply to claims by a non-California resident if the allegedly wrongful conduct occurred in California. *See Hughes v.*

Apple, Inc., No. 22-CV-07668, 2024 WL 4828072, at *3 (N.D. Cal. Nov. 18, 2024). But here, the complaint contains no allegations that any of the unlawful conduct occurred in California. Cook is a Florida resident, and it is reasonable to assume he accessed the Peet’s website while in Florida. The complaint alleges SafeOpt intercepted his browsing activity directly from the website and sent it to Addshoppers, which is based in North Carolina. And there are no allegations that Peet’s made any business decisions relevant to this case—such as the decision to join SafeOpt, or decisions about the marketing emails it would send via SafeOpt—in California. Cook’s CDAFA and CIPA claims are therefore dismissed.

4. *CIPA*. The defendants make a final argument that the CIPA claims should be dismissed because the information intercepted is not the “contents” of communications as required by CIPA. District courts have split on whether browsing history is considered the “contents” of communications. *Compare, e.g., Yoon v. Meta Platforms, Inc.*, 2024 WL 5264041, at *5 (N.D. Cal. Dec. 30, 2024), *with Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082–83 (C.D. Cal. Jul. 15, 2021). Here, at least, it seems clear that the browsing activity intercepted—which included the specific products viewed as opposed to just the IP address and fact that the website was accessed on a particular date—should be considered the “contents” of the communication. Browsing a specific product online is akin to calling the store and asking for information about that product, and everyone agrees that the latter counts as the “content” of the communication.

* * *

The plaintiffs’ CDAFA claims and Cook’s CIPA claim against Peet’s are dismissed. The plaintiffs stated they are no longer pursuing the UCL claims so those are dismissed as well. These claims are dismissed without leave to amend given the case schedule and the fact that plaintiffs have already had a chance to amend. The remaining CIPA claims are not dismissed. Since the briefing on class certification is underway, the defendants may submit a five-page supplemental opposition brief on 2/24/25 and the plaintiffs may submit their reply, with an additional 5 pages, on 3/2/25.

IT IS SO ORDERED.

Dated: February 19, 2025

A handwritten signature in black ink, appearing to read 'V. Chhabria', is positioned above a horizontal line.

VINCE CHHABRIA
United States District Judge